NASA Procedural Requirements

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2016

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology (Revalidated with Change 1, dated May 19, 2011)

Responsible Office: Office of the Chief Information Officer

Appendix A: Definitions

	Term	Definition
A.1	**Authorization to Operate**	The formal acceptance, by an Authorizing Official, that the security of an information system's operation is commensurate with the risk and magnitude of harm resulting from a compromise of that system's confidentiality, integrity, and availability.
A.2	**Boundary Protection**	The security safeguards or countermeasures in place on an information system's logical and physical perimeters.
A.3	**Common Control**	A security safeguard or countermeasure which may be designed, implemented, and assessed at a level which encompasses one or more information systems.
A.4	**Continuous Monitoring**	The ongoing, and often high-frequency, assessment of an information system's security posture usually enabled through the use of automated tools which measure the effectiveness of specific security controls.
A.5	**External Information System**	Any information system which is either owned, or operated by an organization other than NASA, and which processes, maintains, uses, shares, disseminates, or dispositions NASA data.
A.6	**Handbook**	An Agency-level, SAISO-approved document which prescribes the best practices, policies, and procedures regarding various information system security topics.
A.7	**Hybrid Control**	A security safeguard or countermeasure which requires system-specific consideration and may also be partially designed, implemented, and assessed at a level which encompasses one or more information systems.
A.8	**Incident**	Any adverse event or situation associated with a system that poses a threat to the system's integrity, availability, or confidentiality
A.9	**Information Security**	The protection of an information system's confidentiality, integrity, and availability.
A.10	**Information System**	A discrete set of resources designed and implemented for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
A.11	**Internal Information System**	Any information system which is owned and operated by NASA.
A.12	**Least Privilege**	The concept of limiting the flexibility of use an information system user or component has, to the degree necessary to perform a specified role.
A.13	**Management Control**	The collection of supervisory NIST SP 800-53 controls dedicated to information system security.
A.14	**NASA Center**	Any of the collection of facilities and installations designated by NASA, and usually grouped by function (e.g., research, construction, administration).
A.15	**NASA Information**	Any data which is collected, generated, maintained, or controlled on behalf of the Agency.
A.16	**NASA User**	Any explicitly authorized patron of a NASA information system.
A.17	**Near Real-Time (Risk Assessment)**	An analysis of an information system's security posture which closely reflects the immediate state of the system.
A.18	**Non-Digital Media**	Any non-electronic information storage medium (e.g., paper).
A.19	**Ongoing Authorizations**	The continuous acceptance of an information system's operation based on a real-time understanding of the system's security posture.
A.20	**Operational Control**	The collection of strategic NIST SP 800-53 controls dedicated to information system security.

A.21	**Organizationally-Defined Values**	Those details of certain security controls which are meant to be determined by the managing entity. Typically, a memo delivered annually by the OCIO which defines specific details of a security controls implementation.
A.22	**Risk Assessment**	The value-based analysis of an information system's security posture.
A.23	**Risk Management**	A framework defined by NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
A.24	**Security Posture**	The overall state of an information system's confidentiality, integrity, and availability in the face of an ever-changing risk landscape.
A.25	**Technical Control**	The collection of tactical NIST SP 800-53 controls dedicated to information system security.

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS